IN THE UNITED STATES DISTRICT COURT
FOR THE WESTERN DISTRICT OF PENNSYLVANIA

IN THE MATTER OF THE SEARCHES OF: BLUE APPLE IPHONE (**TARGET DEVICE 1**)	Magistrate No. 22-752
BLACK SAMSUNG, IMEI: 352252553061574 (**TARGET DEVICE 2**)	Magistrate No. 22-753

AFFIDAVIT IN SUPPORT OF
AN APPLICATION FOR SEARCH WARRANTS BY TELEPHONE OR OTHER ELECTRONIC MEANS

I, Bryan A. Distelrath, being first duly sworn, hereby depose and state as follows:

INTRODUCTION AND AGENT BACKGROUND

1. I am an investigative or law enforcement officer of the United States within the meaning of Title 18, United States Code, Section 2510(7); that is, an officer of the United States who is empowered by law to conduct investigations of and to make arrests for offenses enumerated in Title 18, United States Code, Section 2516.

2. I have been a Special Agent with the Federal Bureau of Investigation (FBI) since January 2018. During my initial assignment with the FBI, I was assigned to a Health Care Fraud squad, where I investigated complex financial crime that impacted government funded and private insurance programs in the Western District of Pennsylvania. In February 2021, I was assigned to the Greater Pittsburgh Safe Streets Task Force (GPSSTF). GPSSTF is a group of federal, state, and local agencies that work together in the Greater Pittsburgh area to focus investigative resources on violent crimes and related offenses. Prior to my employment with the FBI, I was police officer in Ohio. From 2009 to 2012, I worked as a patrolman for the City of Conneaut Police Department. From 2012 to 2018, I worked for the City of Mentor Police Department as a patrolman and plain clothes detective.

3. As Special Agent with the FBI and a police officer, I have been involved in many narcotics-related arrests and the service of many narcotics-related search warrants. I have handled cooperating sources of information who were involved in narcotics acquisition and/or trafficking. In addition, I have reviewed thousands of communications between drug traffickers as a result of my participation in multiple wiretap investigations. As a result of my narcotics-related training and experience, I am familiar with the methods and language used to distribute narcotics, to launder proceeds, and to operate drug-trafficking conspiracies. As a result of my narcotics-related training and experience, I am familiar with the methods and language used to distribute narcotics, to launder proceeds, and to operate drug-trafficking conspiracies.

4. This application and affidavit are submitted in support of search warrants for cell phones, as described below, associated with JONATHAN YOUNG. Accordingly, law enforcement has probable cause to believe that a search of these locations will produce fruits of, or evidence of, violations of federal felony offenses enumerated in Title 18, United States Code, Section 2516; including, violations of Title 21, United States Code, Sections 841(a)(1) (possession with intent to distribute a controlled substance), 843(b) (unlawful use of a communication facility), 846 (conspiracy); and Title 18, United States Code, Sections 924(c) and 922(g) (firearms violations).

5. As explained below, there is probable cause to conclude that evidence of narcotics trafficking, as well as the illegal possession and/or use of firearms, will be found in cellular telephones associated with YOUNG, which are the subject of the requested search warrants (hereafter occasionally referred to as the "Target Devices").

6. The statements contained in this affidavit are based primarily on discussions with other law enforcement agents and witnesses, information provided to me by other law enforcement agents, review of documents and records, and my personal knowledge, observations, experience

and training. This affidavit is being submitted for the limited and specific purpose of supporting an application for the requested search warrants. I have not, therefore, included every fact known to me concerning the investigation.

IDENTIFICATION OF THE DEVICES TO BE EXAMINED

7. Your Affiant seeks a search warrant for the four electronic storage devices described in Attachment A.

8. These devices have been in secure law enforcement custody since the time they were recovered (the circumstances of which are explained more fully below). In my training and experience, I know that the devices have been stored in which their contents are, to the extent material to this investigation, in substantially the same state as they were when the devices first came into the possession of law enforcement.

PROBABLE CAUSE

9. On February 17, 2022, a search warrant was executed at 11709 Joan Drive, Pittsburgh, Pennsylvania 15235 for the body of JONATHAN YOUNG by law enforcement from the Pittsburgh Bureau of Police (PBP), United States Marshals, and the Western Pennsylvania Fugitive Task Force. YOUNG was taken into custody without incident. YOUNG was wanted for the following Pennsylvania state charges for his involvement in a shooting in the City of Pittsburgh in January 2022:

a. Title 18 § 6105 Person Not to Possess, Use, Manufacture, Control, Sell Or Transfer Firearms;

b. Title 18 § 2702 Aggravated Assault;

c. Title 18 § 2702 Aggravated Assault;

d. Title 18 § 2705 Recklessly Endangering Another Person.

10. PBP Detectives obtained a search warrant for a black Lincoln Aviator (GA CKK7676) that was parked in front of the residence. The vehicle was owned by Enterprise Rentals and rented to YOUNG. The following evidence was recovered from the vehicle:

a. A stolen Tan Glock 19X with automatic conversion kit and extended magazine – recovered from the center console;

b. A small amount of loose marijuana – recovered from the front and rear floorboards;

c. Indicia for YOUNG – recovered from a Gucci bag located in the back seat;

d. Wallet for YOUNG containing numerous bank cards and PA ID Card for YOUNG – recovered from the center console cupholder directly in front of the center console;

e. Blue in color Apple iPhone (**TARGET DEVICE 1**) – recovered from and located directly on top of the wallet in the center console.

11. Detectives interviewed YOUNG's girlfriend, Shealyn Flowers, who was present at the time of arrest. Flowers advised that she didn't have any personal belongings inside of the Lincoln Aviator and denied ownership of the firearm found in the vehicle.

12. On April 27, 2022, YOUNG was indicted in the United States District Court for the Western District of Pennsylvania for:

a. Count 1: 18 U.S.C. 9229(g)(1) and 924(e) – Possession of a Firearm and Ammunition by a Convicted Felon;

b. Count 2: 18 U.S.C. 922(o)(1) – Possession of a Machinegun.

13. On April 29, 2022, at approximately 6:00 a.m., the FBI GPSSTF, with the assistance of the FBI Pittsburgh Special Weapons and Tactics (SWAT) Team, arrived at 11709 Joan Drive, Pittsburgh, Pennsylvania 15235, to arrest YOUNG for his federal arrest warrant. YOUNG was taken

into custody without incident. YOUNG's girlfriend, Shealyn Flowers, and Flower's young daughter were also present in the residence.

14. FBI SWAT personnel observed a firearm in a closet attached to first floor TV/Gaming Room that was easily accessible by any residents in the house.

15. Agents met with Flowers, who signed a FBI Consent to Search form for her residence. The following items were seized:

a. Sig Sauer 9 mm, Serial 5250822, three roads in magazine and one round in the chamber – TV/gaming room, in the closet;

b. Knotted baggies of suspected cocaine base – TV/Gaming Room, in a chair and underneath the cushion;

c. Black Samsung cellular telephone, IMEI: 352252553061574 (**TARGET DEVICE 2**) – Master Bedroom, on makeshift nightstand.

16. Law enforcement tested the suspected cocaine using a Narcotics Identification Kit. The test indicated a positive presence of cocaine.

17. Flowers advised that the black Samsung telephone (**TARGET DEVICE 2**) belonged to YOUNG and the cocaine wasn't hers.

18. **TARGET DEVICE 1** is currently located at Pittsburgh Bureau of Police Zone 5, 1401 Washington Blvd., Pittsburgh, Pennsylvania 15206, and is stored in a secure manner that is designed to preserve the electronic data.

19. **TARGET DEVICE 2** is currently located in the evidence storage facility at the Federal Bureau of Investigation, Pittsburgh Branch, 3311 E. Carson St., Pittsburgh, Pennsylvania 15203, and is stored in a manner that is designed to preserve the electronic data.

20. Your Affiant submits that there is probable cause to search **TARGET DEVICES 1 and 2**.

EVIDENCE COMMONLY GENERATED BY DRUG-TRAFFICKING AND ELECTRONIICALLY STORED IN CELLULAR TELEPHONES AND ELECTRONIC DEVICES

21. Your Affiant is aware through both training as well as experience gained through multiple narcotics investigations, the targets of those narcotics investigations utilize cellular telephones and electronic devices to not only arrange meetings with their drug customers but also speak with fellow co-conspirators as well as their drug sources of supply. Your Affiant is also aware that these targets also utilize multiple cellular telephones and electronic devices at one time in an effort to not only thwart detection by law enforcement but also to compartmentalize their drug trafficking customers to one phone and/or electronic device, their co-conspirators to another phone and/or electronic device, and their drug source of supply to yet another phone and/or electronic device.

22. Based upon my training and experience, I am aware that it is generally a common practice for drug traffickers to store the names and phone numbers of drug customers and photographs and video detailing illegal activities in cellular telephones and electronic devices. Because drug traffickers in many instances will "front" (that is, sell on consignment) controlled substances to their clients, and/or will be "fronted" controlled substances from their suppliers, such record-keeping is necessary to keep track of amounts paid and owed, and such records will also be maintained close at hand so as to readily ascertain current balances. Often drug traffickers keep "pay and owe" records to show balances due for drugs sold in the past ("pay") and for payments expected ("owe") as to the trafficker's supplier(s) and the trafficker's dealer(s). Additionally, drug

traffickers must maintain telephone and address listings of clients and suppliers and keep them immediately available in order to efficiently conduct their drug trafficking business.

23. Persons involved in significant drug trafficking typically conceal within automobiles large amounts of currency, financial instruments, precious metals, jewelry and other items of value, and/or proceeds of drug transactions and evidence of financial transactions relating to obtaining, transferring, secreting, or spending large sums of money derived from narcotic trafficking activities. This type of evidence can also be stored in applications that are commonly found on "SMART" cellular telephones and/or electronic s devices, such as the **TARGET DEVICES** that are referenced throughout this affidavit.

24. Members of Drug Trafficking Organizations (DTO) often take group photographs with other enterprise members posing with paraphernalia, money, firearms and/or drugs. Many cellular telephones have a camera feature that is readily capable of capturing and storing these group photos.

25. Members of DTOs often store each other's phone numbers and contact information in the directories of their cellular phones and/or electronic devices.

26. Based on my experience and familiarity with cellular telephones, I am aware that the telephones have voicemail and telephone directory features, as well as camera features which allow the user to take photographs and store them in the cellular phone's memory card. Based on my experience and training, statements by other law enforcement officers, and personal observations, I know that because of the storage capacity of cellular telephones, the portability of cellular telephones, the ease with which information stored on a cellular telephone may be accessed and/or organized, and the need for frequent communication in arranging narcotics transactions, cellular telephones are frequently used by individuals involved in drug trafficking. In particular,

I and other law enforcement officers have found that information frequently maintained on cellular telephones includes the contact numbers of other co-conspirators, contact numbers for narcotics customers and stored photographs of DTO activities. This evidence will come in the form of caller identification information, call log information, telephone numbers, address information, or other identification information, as well as opened and unopened voicemail and/or text messages, photographs, videos and information about access to the Internet.

27. Members of DTOs routinely use multiple physical phones in succession as one breaks or the DTO feels that the number associated with the phone is compromised to Law Enforcement. The physical phone may no longer be an active communicative device, however many times, these old phones are not discarded as they possess value to the DTO. The replaced device contains within it the contact information for drug customers of the DTO, and many times these phones are maintained as digital phone books should the new active phone become unusable or unavailable. Furthermore, these replaced phones are commonly kept in a relatively accessible location where either all or select members of the DTO can access the information within should it become necessary. As stated above, members of DTOs routinely take photographs and or memorialize other information of evidentiary value within these replaced phones. As such, it is common to recover a multitude of otherwise inactive phones especially at locations central to or important to the DTO.

TECHNICAL TERMS

28. Wireless telephone: A wireless telephone (or mobile telephone, or cellular telephone) is a handheld wireless device used for voice and data communications through radio signals. These telephones send signals through networks of transmitters/receivers, enabling communication with other wireless telephones or traditional “land line” telephones. A wireless

telephone usually contains a "call log," which records the telephone number, date, and time of calls made to and from the phone. In addition to enabling voice communications, wireless telephones offer a broad range of capabilities. These capabilities include: storing names and phone numbers in electronic "address books;" sending, receiving, and storing text messages and e-mail; taking, sending, receiving, and storing still photographs and moving video; storing and playing back audio files; storing dates, appointments, and other information on personal calendars; and accessing and downloading information from the Internet. Wireless telephones may also include global positioning system ("GPS") technology for determining the location of the device.

29. GPS: A GPS navigation device uses the Global Positioning System to display its current location. It often contains records the locations where it has been. Some GPS navigation devices can give a user driving or walking directions to another location. These devices can contain records of the addresses or locations involved in such navigation. The Global Positioning System (generally abbreviated "GPS") consists of 24 NAVSTAR satellites orbiting the Earth. Each satellite contains an extremely accurate clock. Each satellite repeatedly transmits by radio a mathematical representation of the current time, combined with a special sequence of numbers. These signals are sent by radio, using specifications that are publicly available. A GPS antenna on Earth can receive those signals. When a GPS antenna receives signals from at least four satellites, a computer connected to that antenna can mathematically calculate the antenna's latitude, longitude, and sometimes altitude with a high level of precision.

30. Internet: The Internet is a global network of computers and other electronic devices that communicate with each other. Due to the structure of the Internet, connections between devices on the Internet often cross state and international borders, even when the devices communicating with each other are in the same state.

ELECTRONIC STORAGE AND FORENSIC ANALYSIS

31. Based on my knowledge, training, and experience, I know that electronic devices can store information for long periods of time. Similarly, things that have been viewed via the Internet are typically stored for some period of time on the device. This information can sometimes be recovered with forensic tools.

32. As further described in Attachment B, this application seeks permission to locate not only electronically stored information that might serve as direct evidence of the crimes described on the warrant, but also forensic evidence that establishes how each device was used, the purpose of its use, who used it, and when. There is probable cause to believe that this forensic electronic evidence might be on the devices because:

a. Data on the storage medium can provide evidence of a file that was once on the storage medium but has since been deleted or edited, or of a deleted portion of a file (such as a paragraph that has been deleted from a word processing file).

b. Forensic evidence on a device can also indicate who has used or controlled the device. This "user attribution" evidence is analogous to the search for "indicia of occupancy" while executing a search warrant at a residence.

c. A person with appropriate familiarity with how an electronic device works may, after examining this forensic evidence in its proper context, be able to draw conclusions about how electronic devices were used, the purpose of their use, who used them, and when.

d. The process of identifying the exact electronically stored information on a storage medium that are necessary to draw an accurate conclusion is a dynamic process. Electronic evidence is not always data that can be merely reviewed by

a review team and passed along to investigators. Whether data stored on a computer is evidence may depend on other information stored on the computer and the application of knowledge about how a computer behaves. Therefore, contextual information necessary to understand other evidence also falls within the scope of the warrant.

e. Further, in finding evidence of how a device was used, the purpose of its use, who used it, and when, sometimes it is necessary to establish that a particular thing is not present on a storage medium.

50. *Nature of examination*. Based on the foregoing, and consistent with Rule 41(e)(2)(B), the warrant I am applying for would permit the examination of the devices consistent with the warrant. The examination may require authorities to employ techniques, including but not limited to computer-assisted scans of the entire medium, that might expose many parts of the devices to human inspection in order to determine whether it is evidence described by the warrant.

51. *Manner of execution*. Because this warrant seeks only permission to examine devices already in law enforcement's possession, the execution of this warrant does not involve the physical intrusion onto a premises. Consequently, I submit there is reasonable cause for the Court to authorize execution of the warrant at any time in the day or night.

CONCLUSION

52. Based upon the foregoing, I submit that this affidavit supports probable cause for a search warrant authorizing the examination of **TARGET DEVICES 1-2**, as described more fully in Attachment A, to seek the items described in Attachment B.

s/ Bryan A. Distelrath
BRYAN A. DISTELRATH
Special Agent
Federal Bureau of Investigation

Sworn and subscribed before me, by telephone
pursuant to Fed. R. Crim. P. 4.1(b)(2)(A),
this 24th day of May, 2022.

_____
HONORABLE MAUREEN P. KELLY
United States Magistrate Judge

ATTACHMENT A

Property to Be Searched

The items to be searched are:

TARGET DEVICE 1 – Blue Apple iPhone

TARGET DEVICE 2 – Black Samsung cellular phone, IMEI: 352252553061574

The Target Devices will be charged and powered on. The device(s) and all readable and searchable contents will be downloaded to a "CelleBrite" or "XRY" or similar device. The contents downloaded on the "CelleBrite" or "XRY" or similar device will then be copied to a readable computer disc and reviewed by your Affiant or other investigators participating in the investigation. A search warrant return will be provided to the Court thereafter. The **TARGET DEVICES** are currently located in the evidence storage facilities at Pittsburgh Bureau of Police Zone 5, 1401 Washington Blvd., Pittsburgh, Pennsylvania 15206 and the Federal Bureau of Investigation, 3311 E. Carson St., Pittsburgh, Pennsylvania 15203, and are stored in a manner that is designed to preserve the electronic data.

ATTACHMENT B

Particular Items to be Seized

1. All records on the Target Devices described in Attachment A that relate to drug trafficking in violation of 21 U.S.C. §§ 841(a)(1), 843(b), and 846, and firearms offenses in violation of 18 U.S.C. §§ 924(c), 922(g) including:

a. Evidence of communications referring to or relating to illegal narcotics or narcotics trafficking, including records of telephone calls, emails, instant messaging, or other records of communications, and including the identity of phone numbers, email accounts, or other electronic accounts used for such communications;

b. Evidence of communications with suppliers, purchasers, prospective suppliers, or prospective purchasers of illegal narcotics, including records of telephone calls, emails, instant messaging, or other records of communications, and including the identity of phone numbers, email accounts, or other electronic accounts used for such communications;

c. Evidence of communications referring to or relating to firearms and/or ammunition, including records of telephone calls, emails, instant messaging, or other records of communications, and including the identity of phone numbers, email accounts, or other electronic accounts used for such communications;

d. Documents, including photographs and video, depicting illegal narcotics, drug paraphernalia, firearms, or ammunition;

e. Documents, including video and/or audio recordings, discussing and/or referring to illegal narcotics, drug paraphernalia, firearms, or ammunition;

f. Documents, including photographs and video, depicting illegal narcotics, drug paraphernalia, firearms, ammunition, violence relating to firearms or ammunition;

g. Any and all information revealing the identity of co-conspirators in drug trafficking and/or firearm-related activity;

h. Any and all bank records, transactional records, records of wire transfers, checks, credit card bills, account information, and other financial records;

i. Any and all information suggesting sudden or unexplained wealth and/or unidentified conspirators;

j. Any and all information identifying the sources of supply and/or unidentified conspirators may have secured illegal narcotics, drug paraphernalia, firearms, and/or ammunition; and

k. Any and all information recording the scheduling of travel and/or unidentified conspirators, including destinations, dates of travel, and names used during travel.

2. All text messaging, call logs, emails, and/or other records of communication relating to the planning and operation of the above-specified drug trafficking and firearms offenses.

3. Evidence of user attribution showing who used, owned, or controlled Target Devices at the time the things described in this warrant were created, edited, or deleted, such as logs, registry entries, configuration files, saved usernames and passwords, documents, browsing history, user profiles, email, email contacts, "chat," instant messaging logs, photographs, and correspondence.

4. Evidence of software that would allow others to control the Target Devices, such as viruses, Trojan horses, and other forms of malicious software, as well as evidence of the presence or absence of security software designed to detect malicious software.

5. Evidence of the lack of such malicious software.

6. Evidence indicating how and when the Target Devices were accessed or used to determine the chronological context of the Target Devices access, use, and events relating to the crimes under investigation and to the Target Devices' user.

7. Evidence indicating the Target Devices user's state of mind as it relates to the crime under investigation.

8. Evidence of the attachment to the Target Devices of other storage devices or similar containers for electronic evidence.

9. Evidence of counter-forensic programs (and associated data) that are designed to eliminate data from the Target Devices.

10. Evidence of the times the Target Devices was used.

11. Evidence of how the Target Devices were used and the purpose of its use including firewall logs, caches, browsing history, cookies, "bookmarked" or "favorite" web pages, temporary Internet directory or "cache," search terms that the user entered into any Internet search engine, records of user-typed web addresses, and other records of or information about the Target Devices' Internet activity.

12. Records of or information about Internet Protocol addresses used by the Target Devices.

13. Passwords, encryption keys, and other access devices that may be necessary to access the Target Devices.

14. Documentation and manuals that may be necessary to access the Target Devices or to conduct a forensic examination of the Target Devices.

15. Contextual information necessary to understand the evidence described in this attachment.

16. All serial numbers or International Mobile Equipment Identity (IMEI) numbers associated with any cellular telephones.

17. Log files, contact information, phone books, voicemails, text messages, draft messages, other stored communication, calendar entries, videos, and photographs related to matters described above.

In searching the Target Devices, the federal agents may examine all of the information contained in the Target Devices to view their precise contents and determine whether the Target Devices and/or information fall within the items to be seized as set forth above. In addition, they may search for and attempt to recover "deleted," "hidden," or encrypted information to determine whether the information falls within the list of items to be seized as set forth above.

As used above, the terms "records" and "information" includes all forms of creation or storage, including any of the following:

a. Any form of computer or electronic storage (such as hard disks or other media that can store data);

b. Text messages or similar messages such as SMS or IM, saved messages, deleted messages, draft messages, call logs, all phone settings (*i.e.* call, messaging, display), priority senders, photographs, videos, links, account information, voicemails and all other voice recordings, contact and group lists, and favorites;

c. Pictures, all files, cloud files and relevant data without password access, storage information, documents, videos, programs, calendar information, notes, memos, word documents, PowerPoint documents, Excel Spreadsheets, and date and time data;

d. Payment information, to include account numbers, names, addresses, methods of payment, amounts, additional contact information, and financial institutions;

e. Lists and telephone numbers (including the number of the phone itself), names, nicknames, indicia of ownership and/or use, and/or other contact and/or identifying data of customer, co-conspirators, and financial institutions;

f. Applications (Apps), to include subscriber information, provider information, login information, contact and group lists, favorites, history, deleted items, saved items, downloads, logs, photographs, videos, links, messaging or other communications, or other identifying information;

g. Social media sites to include, name and provider information of social media network(s), profile name(s), addresses, contact and group lists (*i.e*. friends, associates, etc.), photographs, videos, links, favorites, likes, biographical information (*i.e*. date of birth) displayed on individual page(s), telephone numbers, email addresses, notes, memos, word documents, downloads, status, translations, shared information, GPS, mapping, and other information providing location and geographical data, blogs, posts, updates, messages, or emails;

h. Any information related to co-conspirators (including names, addresses, telephone numbers, or any other identifying information);

i. Travel log records from GPS data (*i.e.* Google Maps and/or other Apps), recent history, favorites, saved locations and/or routes, settings, account information, calendar information, and dropped pinpoint information;

j. Internet service provider information, accounts, notifications, catalogs, Wi-Fi information, search history, bookmarks, favorites, recent tabs, deleted items and/or files, downloads, purchase history, photographs, videos, links, calendar information, settings, home page information, shared history and/or information, printed history and/or information, or location data;

k. Email data, including email addresses, IP addresses, DNS provider information, telecommunication service provider information, subscriber information, email provider information, logs, drafts, downloads, inbox mail, sent mail, outbox mail, trash mail, junk mail, contact lists, group lists, attachments and links, and any additional information indicative of the above-specified offenses.

The term "computer" includes all types of electronic, magnetic, optical, electrochemical, or other high speed data processing devices performing logical, arithmetic, or storage functions, including desktop computers, notebook computers, cellular telephones, tablets, server computers, and network hardware.